WEBINAR #4

Internet Society
Cybersecurity SIG

Why National Cybersecurity Awareness Programmes Often Fail

October 15 2020
12:00 EDT | 16:00 UTC

Speaker:
Dra. Eva Nagyfejeo
Global Cybersecurity Capacity Centre – Oxford Martin School

#CyberSecMonth

Why national cybersecurity awareness programmes often fail

October 15 2020

Oscar Noe Avila
Let's start. Good afternoon, everyone, or good morning, depending on where you are watching us from. Welcome to the fourth session of the Global Cybersecurity Forum. My name is Oscar Avila. I am the current president of the ISOC Cybersecurity SIG. And I'm delighted to kick off this session, Why National Cybersecurity Awareness Programmes Often Fail.

I would like to make a couple of announcements. Please keep your mic off during the session, and use the chat feature to formulate your questions and comments. We will have a q&a session at the end of the webinar, at least we will have 15 minutes for questions.

I am delighted to introduce Dr. Enrico Calandro, he's our moderator today. Enrico is the co-director of the Cybersecurity Capacity Center of South Africa, and member of the advisory board of the Global Forum on Cyber Expertise. Enrico, the floor is yours.

Enrico Calandro
Thank you. Thank you very much Oscar. Hi everyone.

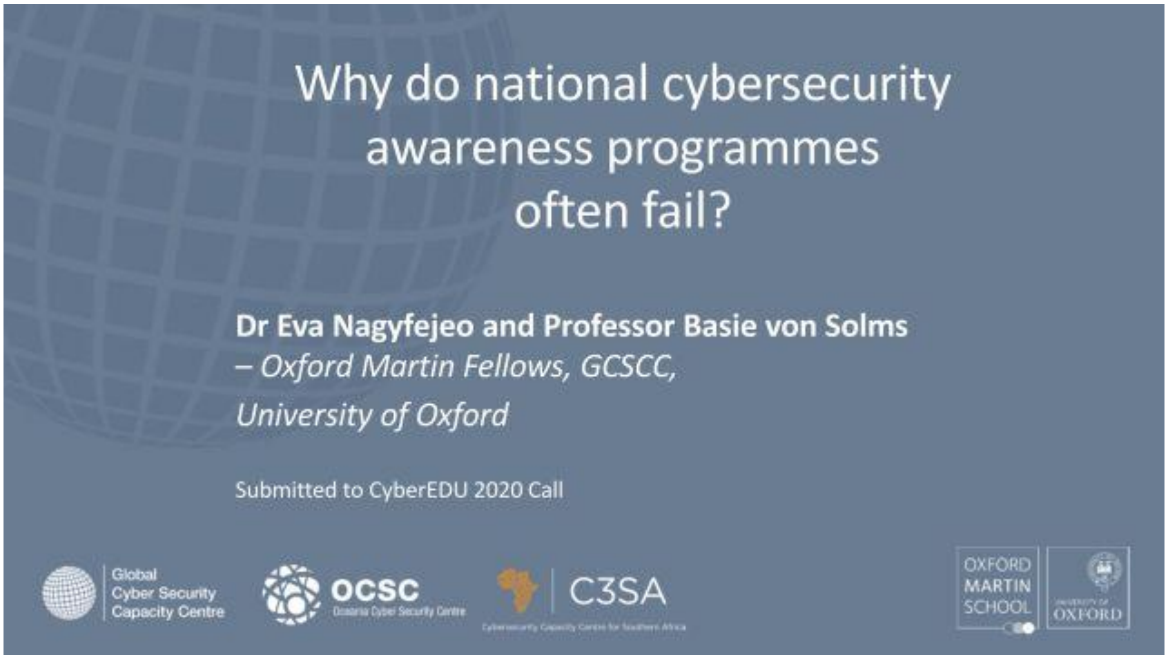
I'm delighted, actually, to be moderating this panel. I think it's going to be a very interesting one, because, as you probably are all aware, October is the month of cyber awareness all over the world. So, I think that the discussion is really pertinent to this period of the year.

We have with us a great speaker, and a colleague, from the Global Cyber Security Capacity Center at the Oxford University. Her name is Dr. Eva Nagyfejeo. Eva is a research fellow at this Global Center at University of Oxford, where she supports the delivery of global cybersecurity capacity building expertise, by promoting the center's Cyber Maturity Model (CMM) for nations, which is a methodology that she's going to describe as well, and through these country reviews. By the end of last year, 2019, she participated in nine country reviews around the world. So, her research is actually based on field work, where Eva has really engaged with a number of stakeholders, she met them in person, and she has collected the data in person. So, I think it would be great if Eva maybe can share that experience, because it's really valuable. And currently, she is leading the CMM revision project.

The research she's going to present, as Oscar said, the title is Why Do National Cybersecurity Awareness Programmes Often Fail. So, not always, but often, unfortunately, they fail. We will try to understand why, and it's based on eight cyber maturity assessments across three continents, so it's really a global study. The data was collected between 2017 and 2018 and, as I said, Eva was part of a number of these CMM reviews. So, she's going really to provide us that kind of academic expertise, but also direct experience in conducting these kind of studies.

So, without any further ado, Eva, the microphone is yours, and we look forward to your presentation. Thank you.

Eva Nagyfejeo
Thank you very much, Enrico and Oscar for introduction. Welcome, everyone. Thanks very much for joining us today.



Why do national cybersecurity awareness programmes often fail?

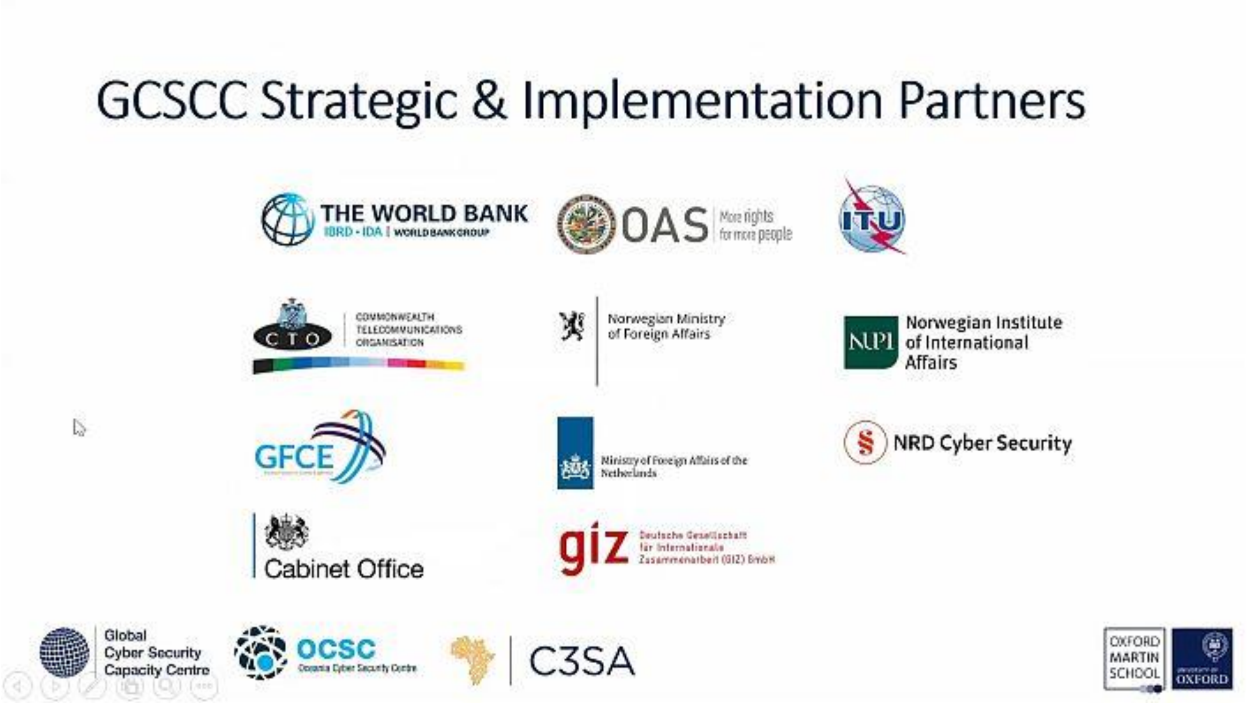
Dr Eva Nagyfejeo and Professor Basie von Solms
– Oxford Martin Fellows, GCSCC,
University of Oxford

Submitted to CyberEDU 2020 Call

Global Cyber Security Capacity Centre
OCSC Oceania Cyber Security Centre
C3SA
Cybersecurity Capacity Centre for Southern Africa
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD

And I'm very honored to be here with you and I'm very happy to present to you the paper that Professor Basie von Solms and I wrote together, focusing on why do national cybersecurity awareness raising programs often fail.

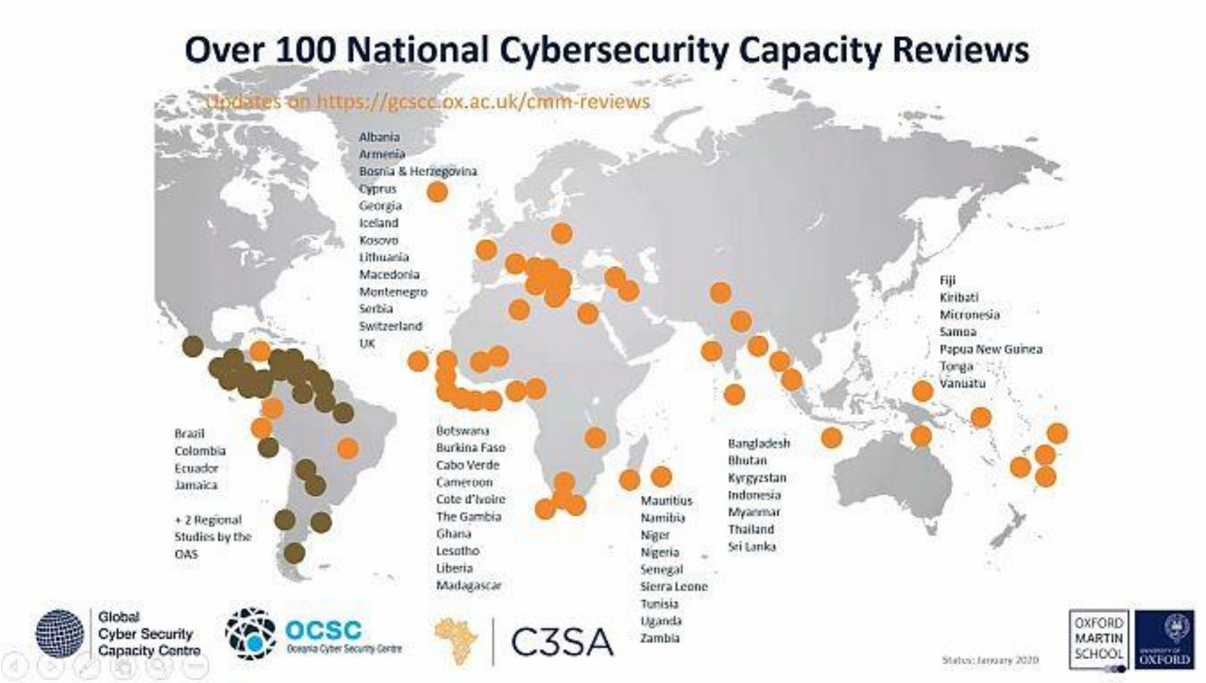
To give you a little background behind the idea of the paper, first I would like to explain to you the work of the Global Cyber Security Center. So, the center was launched in 2014, with the aim of developing a cyber maturity model to assess the country's cybersecurity capacity, and the research team at the time were together with strategic and implementation partners.



GCSCC Strategic & Implementation Partners

THE WORLD BANK
IBRD · IDA | WORLD BANK GROUP
OAS More rights for more people
ITU
CTO COMMONWEALTH TELECOMMUNICATIONS ORGANISATION
Norwegian Ministry of Foreign Affairs
NUPI Norwegian Institute of International Affairs
GFCE
Ministry of Foreign Affairs of the Netherlands
NRD Cyber Security
Cabinet Office
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
Global Cyber Security Capacity Centre
OCSC Oceania Cyber Security Centre
C3SA
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD

As you can see on the slide, we have a number of cyber capacity building partners, who supported the development of the Cyber Maturity Model, and also supporting the development of the CMM across the different regions of the world, such as the World Bank, the OAS, the ITU, the UK front office. And we have also working together with the Oceania Cyber Security Center in Australia, and also the recently launched Cyber Capacity Center in South Africa.



Over 100 National Cybersecurity Capacity Reviews

Updates on https://gcscc.ox.ac.uk/cmm-reviews

Albania
Armenia
Bosnia & Herzegovina
Cyprus
Georgia
Iceland
Kosovo
Lithuania
Macedonia
Montenegro
Serbia
Switzerland
UK

Fiji
Kiribati
Micronesia
Samoa
Papua New Guinea
Tonga
Vanuatu

Brazil
Colombia
Ecuador
Jamaica

+ 2 Regional Studies by the OAS

Botswana
Burkina Faso
Cabo Verde
Cameroon
Cote d'Ivoire
The Gambia
Ghana
Lesotho
Liberia
Madagascar

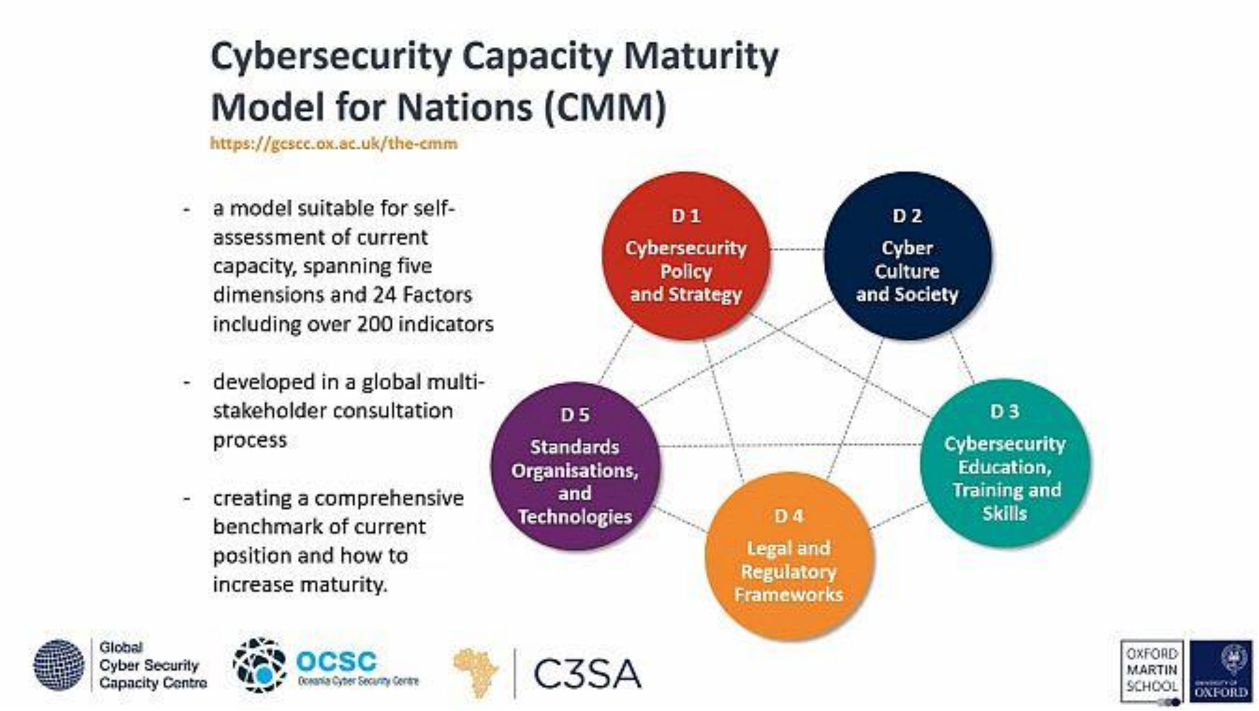
Mauritius
Namibia
Niger
Nigeria
Senegal
Sierra Leone
Tunisia
Uganda
Zambia

Bangladesh
Bhutan
Kyrgyzstan
Indonesia
Myanmar
Thailand
Sri Lanka

Status: January 2020

Global Cyber Security Capacity Centre
OCSC Oceania Cyber Security Centre
C3SA
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD

And this map shows you that in the past five years, the Cyber Capacity Center was quite busy, along with its implementation partners. This project reached over 100 national cyber security reviews. If anybody would like to learn more about the center and model, I would like to encourage you to please visit the website, our new website, gcscc.ox.ac.uk.



Cybersecurity Capacity Maturity Model for Nations (CMM)

https://gcscc.ox.ac.uk/the-cmm

- a model suitable for self-assessment of current capacity, spanning five dimensions and 24 Factors including over 200 indicators
- developed in a global multi-stakeholder consultation process
- creating a comprehensive benchmark of current position and how to increase maturity.

D 1 Cybersecurity Policy and Strategy

D 2 Cyber Culture and Society

D 3 Cybersecurity Education, Training and Skills

D 4 Legal and Regulatory Frameworks

D 5 Standards Organisations, and Technologies

Global Cyber Security Capacity Centre

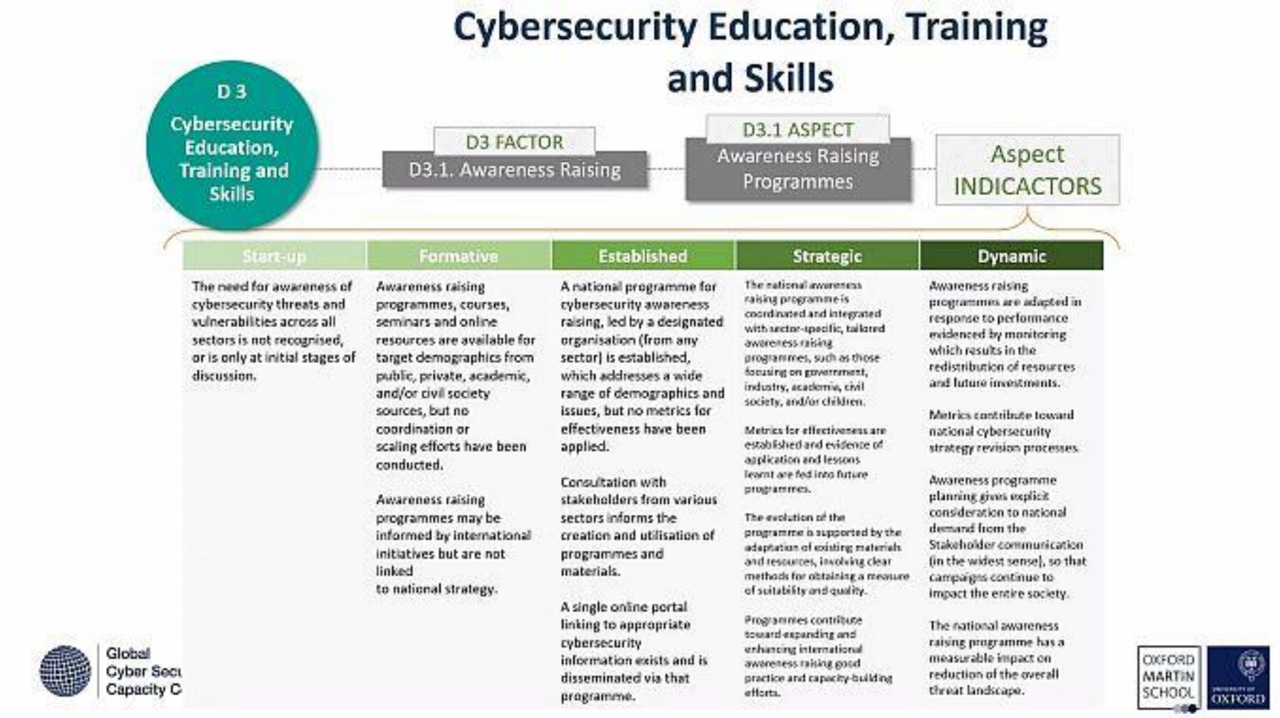
OCSC Oceania Cyber Security Centre

C3SA

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

And since, in the past five years, we collected a lot of data from CMM reviews, the main question that drove the paper was, can we identify main challenges, emerging themes, when countries have to develop national awareness raising programmes? To what extent are these challenges similar? To what extent do they differ from each other? And, when we go to the country and deploy the Cyber maturity model, we focus on five main areas, for five main dimensions, and one of the dimensions is focuses on cybersecurity awareness raising programs, or cybersecurity education and training and skills. And within the D3, the cyber security awareness raising programs that we looked more deeply into the in the paper.



Cybersecurity Education, Training and Skills

D 3 Cybersecurity Education, Training and Skills

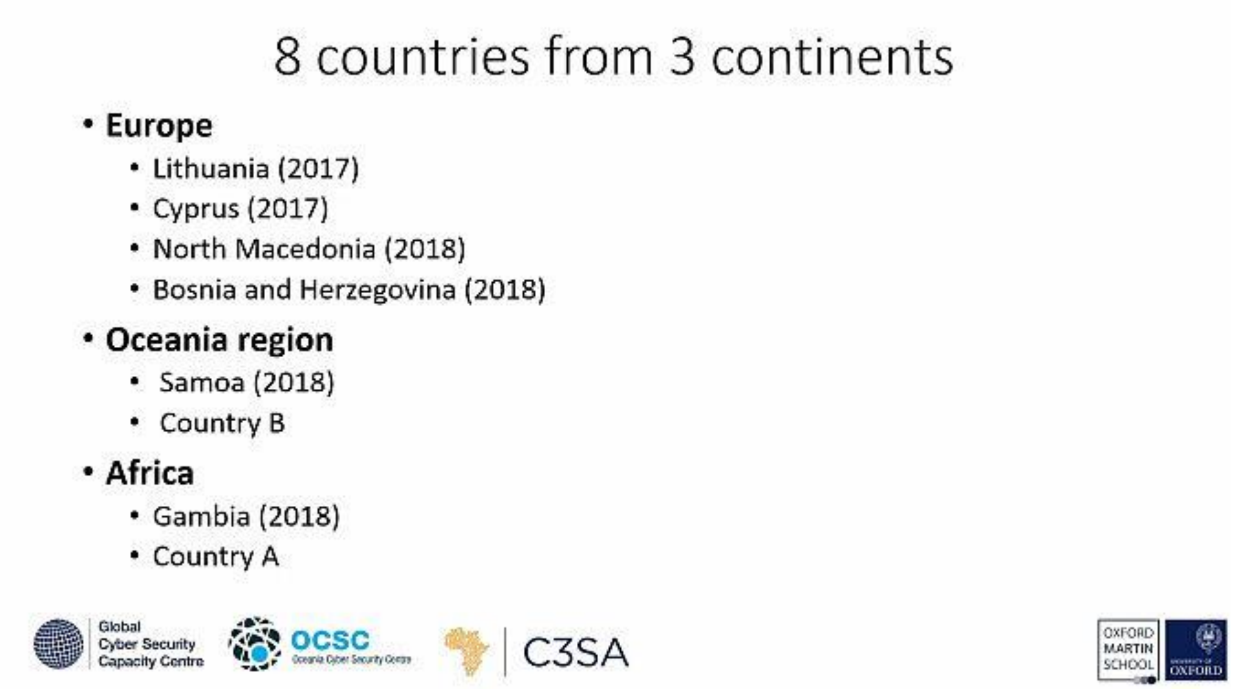
D3 FACTOR
D3.1. Awareness Raising

D3.1 ASPECT
Awareness Raising Programmes

Aspect INDICACTORS

Start-up	Formative	Established	Strategic	Dynamic
The need for awareness of cybersecurity threats and vulnerabilities across all sectors is not recognised, or is only at initial stages of discussion.	Awareness raising programmes, courses, seminars and online resources are available for target demographics from public, private, academic, and/or civil society sources, but no coordination or scaling efforts have been conducted. Awareness raising programmes may be informed by international initiatives but are not linked to national strategy.	A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) is established, which addresses a wide range of demographics and issues, but no metrics for effectiveness have been applied. Consultation with stakeholders from various sectors informs the creation and utilisation of programmes and materials. A single online portal linking to appropriate cybersecurity information exists and is disseminated via that programme.	The national awareness raising programme is coordinated and integrated with sector-specific, tailored awareness raising programmes, such as those focusing on government, industry, academia, civil society, and/or children. Metrics for effectiveness are established and evidence of application and lessons learnt are fed into future programmes. The evolution of the programme is supported by the adaptation of existing materials and resources, involving clear methods for obtaining a measure of suitability and quality. Programmes contribute toward expanding and enhancing international awareness raising good practice and capacity-building efforts.	Awareness raising programmes are adapted in response to performance evidenced by monitoring which results in the redistribution of resources and future investments. Metrics contribute toward national cybersecurity strategy revision processes. Awareness programme planning gives explicit consideration to national demand from the Stakeholder communication (in the widest sense), so that campaigns continue to impact the entire society. The national awareness raising programme has a measurable impact on reduction of the overall threat landscape.

So here, I would like to give you a very short snapshot of the model, I'm not going to go very much into detail. But each dimension consists of factors. Each factor consists of aspects and indicators, a set of indicators that spread across five stages of maturity, from startup to dynamic. And here you can see the indicators that we use when asking questions regarding the national awareness raising program in the country. So, we asked from the cyber experts, and the different stakeholders, when we deployed the CMM with the research team, with regards to whether the country has a national program for cybersecurity awareness raising, whether they have a designated organization that supervises these programs, to what extent they consulted with different stakeholders when developing the program. Do they have awareness raising courses, seminars, online resources available? Who are the owners of these campaigns? Do they cooperate together or not? So, these are the indicators that we use, and framing to questions, when we do the focus group discussions.

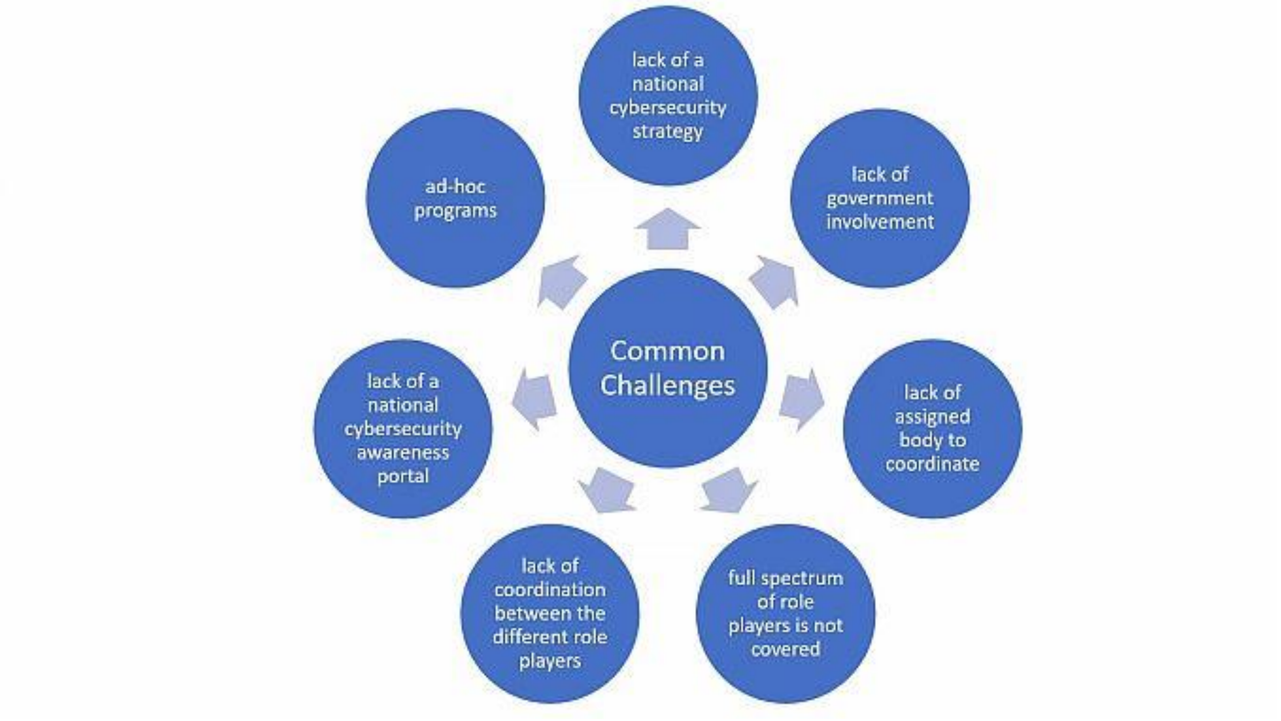


8 countries from 3 continents

- **Europe**
  - Lithuania (2017)
  - Cyprus (2017)
  - North Macedonia (2018)
  - Bosnia and Herzegovina (2018)
- **Oceania region**
  - Samoa (2018)
  - Country B
- **Africa**
  - Gambia (2018)
  - Country A

Global Cyber Security Capacity Centre
OCSC
Oceania Cyber Security Centre
C3SA
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD

So, we picked eight countries from three continents for that data analysis, and the reason behind picking these eight countries were their geographical location, they were located on three different continents. And, we were very interested to see whether they are similar patterns, similar challenges, that these countries have to face when they develop an awareness raising program. So, we picked four countries from Europe, Lithuania, and Cyprus, they're two EU countries, and two from the western Balkans, North Macedonia and Bosnia Herzegovina, I also had the opportunity to be part of the research team deploying the CMM in these two countries. Also, we picked two countries in the Oceania region, Samoa and Country B, and two countries in Africa, Gambia and Country A. The reason that the two countries are not referenced is because their review reports, CMM reports, haven't been published, and because of that, we not going to mention their names. The dates indicate when the CMM reports of these countries were published, and we tried to analyze the data collected during the CMM reviews, and also from the CMM reports, at the time of the assessment. The main conclusion and observations that we made is that these cybersecurity awareness raising programmes in these countries are often led by different owners, who do not have the adequate resources in place to implement these campaigns, and they do not really coordinate with each other, therefore creating a fragmentation in the national awareness raising programme in the countries. So, despite the differences in geographical locations, interestingly, these countries still face similar challenges, similar issues with regards to national awareness raising programs.


Common Challenges
lack of a national cybersecurity strategy
lack of government involvement
lack of assigned body to coordinate
full spectrum of role players is not covered
lack of coordination between the different role players
lack of a national cybersecurity awareness portal
ad-hoc programs

We tried to divide the challenges into seven main areas of concern. The first is that, at the time of the assessment, most of the countries have a cybersecurity strategy in place, and having a cybersecurity strategy indicates that the government is really supporting existing programs. So, because if there were no strategy, there was not enough government support for the available awareness raising programs. Also, in the public CMM reports in Lithuania, North Macedonia, Bosnia Herzegovina, and Samoa, they indicated that these awareness raising campaigns that are available in these countries are driven by different stakeholders, but they were still not linked to the country's support efforts, the national Cybersecurity strategy, if there was cybersecurity strategy in place at the time.

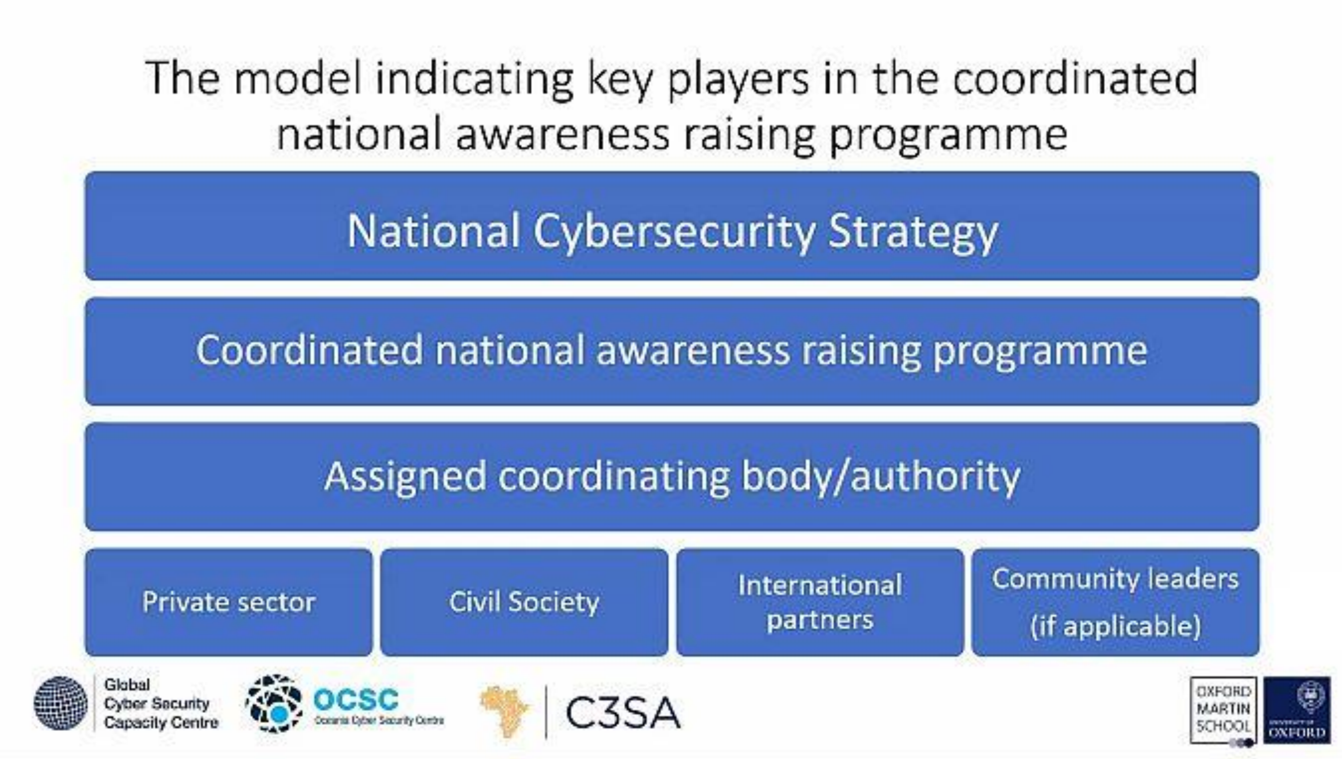
Also, none of these countries at the time of the assessment, 2017 and 2018, had an assigned body, whether it's a ministry or an agency in place, who would supervise and implement the awareness raising program in the country at the national level. Having a body and organization in place, who would coordinate, would have to avoid duplication and overlaps among the existing programs.

Also, we observed that there were not enough coordination between the different role players active in the cybersecurity awareness raising programmes in the country. So, based on our experience, when we asked questions from different stakeholder groups, from the focus group discussions, some of them are not even aware of what other awareness raising programs are available in these given countries. Also, none of these countries, at the time of the assessment, had a national cybersecurity awareness worker in place, that would act as a single point of [inaudible], and promote cybersecurity, maturity, cybersecurity awareness related materials and resources, to the public. And also, the existing programs did not really cover the full spectrum of the role players who were involved in these programmes, whether they included the government, or the private sector, universities, and schools, and civil societies.

So, these were very interesting observations we made and, of course, it's also important to talk a bit about the differences as well, because there were also cultural differences, with regards to how these countries, and the public, dealt with cybersecurity issues. So, for instance, in African countries, like the countries I had the opportunity to do the assessments, they have culture towards forgiveness. And if, for instance, a young girl would become a victim of cyber bullying, they would rather forgive their offenders, than to report it to the police, for instance. So, there are also cultural issues that needs to be taken into consideration in certain areas and regions, and countries, when developing awareness raising programmes. So, to make sure that, to help, to change the mindset, and also to promote the reporting channels that are available for victims of cyber abuse, and cyber bullying, or or cyber fraud, for instance.

And, also there are the issues regarding the language barriers, as well. Most of the countries in South America, in Asia, and in the Oceania region as well, if the awareness raising materials are available in English, and English is not the primary language of the population, especially in African countries, then it's very difficult to promote cybersecurity awareness raising among the population. So, these are also other issues that need to be taken into consideration, when developing awareness raising programmes as well.

And the other things that were mentioned by participants, during the focus group discussions, is the lack of political leadership with regards to cybersecurity. Another suggestion to remedy this problem could be to maybe provide workshops to the parliamentarians, to raise awareness on cybersecurity issues. Also, another suggestion could be, in the time of the COVID-19 pandemic, to design online materials to the parliamentarians, that they are obliged to take. So, if the country doesn't have the driving force, at the top level, to make cybersecurity a priority, and promote awareness and cybersecurity, if it's very difficult to build this resilience in the society, to help and establish responsible behavior online.



The model indicating key players in the coordinated national awareness raising programme

National Cybersecurity Strategy

Coordinated national awareness raising programme

Assigned coordinating body/authority

Private sector

Civil Society

International partners

Community leaders (if applicable)

Global Cyber Security Capacity Centre

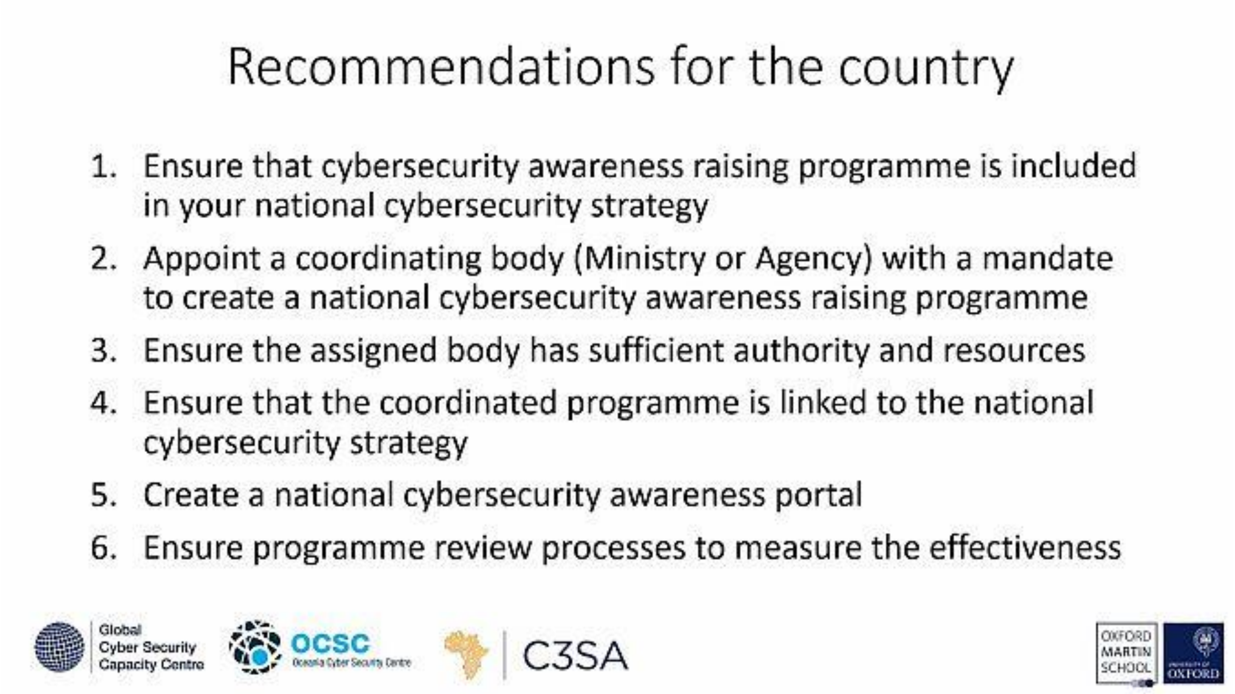
OCSC Oceania Cyber Security Centre

C3SA

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

And we came up with a high level model, as you can see on the slide, for that has four levels, and with some general guidelines for the country to to develop a national awareness raising program. We always try to emphasize the need to have an assigned coordinating body, and also emphasized the need for a multistakeholder approach. So, when the government is developing a program, we would always like to emphasize the need to involve different stakeholders, the private sector, the civil society, the international partners, and, if applicable, also the community leaders. The community leaders were put there because, based on my experience going to countries in the Oceania region, also in the African countries, it was very interesting to see the crucial role that community leaders, and also religious leaders play in society. So, for instance, in Samoa, I think they call the village chiefs, the matais, they have a very important role to shape the way the community thinks about certain issues. Also, in my experience, when we did an assessment in an African country, and we asked the stakeholders whether they think that the church could play a role in raising awareness, cybersecurity of an increasing amount of public, and they said definitely, that would be great, and it was a very interesting experience, that meeting as well, the importance to involve them in countries where the community leaders, and in those religious countries, where they have an important role to influence communities, and maybe the local communities will listen to them more than other members of the public, for instance.



Recommendations for the country

1. Ensure that cybersecurity awareness raising programme is included in your national cybersecurity strategy
2. Appoint a coordinating body (Ministry or Agency) with a mandate to create a national cybersecurity awareness raising programme
3. Ensure the assigned body has sufficient authority and resources
4. Ensure that the coordinated programme is linked to the national cybersecurity strategy
5. Create a national cybersecurity awareness portal
6. Ensure programme review processes to measure the effectiveness

We came up with some recommendations for the country, to develop an awareness raising programme. So, the first would be to develop cybersecurity strategy. In the case they don't have a cybersecurity strategy in place, they could still come up with a coordinated awareness raising program, that would be later linked back to the cybersecurity strategy, and as an action plan. It's very important in this report, to involve different stakeholders, the private sector, civil society, and international stakeholders, or at least listen to them, because they can bring a lot of expertise to the development of the programme, and maybe share experiences and challenges that neighboring countries have planned, in financing the bank's raising programs.

The next suggestion for us, with the country, would be to appoint an agency, as an organization, whether it's a ministry or agency, to create, or at least coordinate and supervise the existing governance raising programs, in order to make sure that the owners of the campaigns have a clear understanding of their roles and responsibilities, in order to avoid duplication, and also to make sure that the resources are going into, and allocated into the right campaigns. Also, we suggested to ensure that the assigned body has sufficient authority and resources to implement this, and coordinate among existing programs. Also, we suggested to create a national awareness raising portal, which would act as a single point of contact to disseminate materials, seminars, to the public, to everyone in -- it would be better if it will be in the local language, as well, not just English.

And, of course, we shouldn't forget about the programme review processes, in order to make sure to what extent the programmes are effective, if there's anything lacking, also, taking into consideration the emerging threats, that should be reviewed time to time, and inform strategy decision making, and feedback into the strategy and awareness raising programs. So, it would be a periodic review process.

So, these are our general guidelines for the country to develop a cybersecurity -- a coordinated cybersecurity awareness raising program.

Role of international stakeholders

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP
ITU
OAS
More rights for more people
GFCE
Get Safe Online
APWG
UNDP
OSCE
FIRST
CTO
COMMONWEALTH TELECOMMUNICATIONS ORGANISATION
ECOWAS
CEDEAO
asean
Global Cyber Security Capacity Centre
OCSC
Oceania Cyber Security Centre
C3SA
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD

And the role of the international stakeholders cannot be emphasized enough. Just mentioning a few, but many, many international actors have already been actively involved in engaging in cyber capacity building activities around the world, such as Get Safe Online, OAS, ITU, World Bank, ASEAN, OSCE with the CBM measures, so just to mention a few. They have a very important role, and they could also advise governments, group with other partners, and they could also save some time spending on developing an awareness raising program, because they can share the experience and expertise as well.

Visit Cybil.

www.cybilportal.org
#CybilPortal

GFCE
ASPI Australian Strategic Policy Institute
DiPLO
FIRST
Global Cyber Security Capacity Centre
NUPI Norwegian Institute of International Affairs

Last year, at Addis Ababa, during the GFCE annual meeting, the Cybil Portal was launched, which is globally owned, and it serves as a one stop knowledge hub, providing information on cyber capacity building projects, tools, and publications. So, if anyone of you is interested to learn more about the cyber capacity building projects, and materials. I would encourage you to please check out these websites.

And to a conclusion, we concluded in the paper that the fundamental challenges, with regards to national cybersecurity awareness raising, remains the same regardless of the geographical differences between the countries. No country is immune to cyber risk, and we don't need to reinvent the wheel with regards to existing frameworks, but countries need a plan, and they need a coordinated approach to national awareness raising programmes, and they need to put forward a plan to help individuals to become more confident to control their activities online, especially nowadays, as a result of the COVID-19 pandemic. and we are required to work from home, and shift to remote work. During these challenging times, digital education is rising, and also, it gives us more vulnerability to the cyber criminals, and cyberattacks directed at staff, and different sectors, including academic students, schools, and become victims of email scams at large. So, I think it's even more important nowadays for governments to have a priority on cybersecurity awareness raising programmes.

Thank you!

Global
Cyber Security
Capacity Centre

Department of Computer Science
University of Oxford
15 Parks Road, Oxford, OX1 3QD, UK
Phone: +44(0)1865 287903
cybercapacity@cs.ox.ac.uk

www.oxfordmartin.ox.ac.uk/cybersecurity

@CapacityCentre

https://www.linkedin.com/company/
global-cyber-security-capacity-centre/

So that would be my presentation, and thank you very much for listening, and I'm looking forward to the discussion, and the questions.

Enrico Calandro
Thank you very much Eva, for this really interesting presentation, and for sharing with us this very informative research.

So, before giving the floor to the audience, there are a number of points that I would like to discuss with you, that triggered my interest in these issues. So, I think one of the main points that you raised is on this lack of coordination, right? And the fact that there is a need of having a body, or an entity, at the government level, that somehow coordinates a good cyber awareness programme. But, at the same time, you also said that one of the main problems, actually of the fact that there isn't a coordination bodies, that probably there is lack of political leadership, broadly on cybersecurity, and then also specifically on cyber and awareness. So, I'm wondering also, maybe one of the reasons for this lack of political leadership, is that a number of members of parliament, or other policymakers, actually do not have enough knowledge of cybersecurity in the country, and do not understand how to prioritize on that, how to budget on cybersecurity, and how to develop a strategy, and so on, and so forth. So, I'm just wondering, what do you think of the Cyber Maturity Model for Nations report, to be used as an awareness tool for policymakers, to really, you know, build their capacity, so that then they can develop this kind of political leadership, that would somehow coordinate a proper cyber awareness programme? So is the

CMM an awareness tool for policymakers at the national level, what do you think about that, based on your experience?

Eva Nagyfejeo
Yeah, thank you very much for the question, Enrico, this is a very relevant question. And indeed, the the CMM reports that we write together, it's also, as you mentioned very well, it's a tool for the decision maker, to raise awareness of the cybersecurity issues. Actually, when we conduct a review in the country, when we go there with the research team in person, we ask for recommendations as well from the stakeholders, what they think is lacking in the country, and providing the expertise and knowledge, while we deployed the CMM, we have a better understanding of the gaps in cybersecurity capacity in the country, whether it's awareness raising, whether it's the legal frameworks, various technology, strategy, problems, cultural issues, as well.

So, when we deliver the CMM reports, in consultation with the ministry in charge, we always provide recommendations, what are the next steps to reach the next stages of maturity. And it's also true for the awareness raising program, so the CMM report is in a way an awareness raising tool, and we really hope that the CMM reports could help to raise awareness within the government. And I think, once we go in to conduct second CMM reviews, now we had the second one in Uganda recently, and then we had another second CMM review in Kosovo, as well, we will see the developments in the past four years, where the country is, how the country put forward, or to what extent they agreed on the recommendation. So, we provide some guidelines what to do, but it's always up to the country to decide, and the decision makers, how they want to move forward to reach the next stage of maturity.

Enrico Calandro
Thank you, thank you very much, Eva. I see in the chat a few questions. So, the first one is from Miguel Garces, I don't know if Miguel, would you like to ask the question yourself? If you can unmute yourself, or otherwise, I can ask that on your behalf.

Miguel?

Okay. So, it's a very interesting question. He's asking, Have you come across any data suggesting that cyber criminals are targeting, and/or using, countries with less mature cyber maturity?

Eva Nagyfejeo
Hmm.

Enrico Calandro
Is there enough evidence on that? I think is a very interesting question.

Eva Nagyfejeo
Yeah, that's a very interesting question. I don't think I came across that in this part. I would be very interested to look at, and maybe, if there is any statistics available, I think it could be a very good research paper actually to write on. And, I mean, if the country has less capacity in terms of cybersecurity maturity, we would assume that they are more vulnerable. But, it would be very interesting to see through data, and look at it more closely.

Thank you very much for the question.

Enrico Calandro
Yeah, absolutely. I think it's a very interesting one.

Enrico Calandro
There is another question from Aireni Omerri. Aireni, would you like to ask your question yourself, or should I ask on your behalf?

Enrico Calandro
Maybe I can ask this question as well.

Eva, from the research that you have done, which countries in the global south have successfully implemented National Cybersecurity Awareness programs? Is there any country that you can recall where you've seen an example of a successful cyber awareness program? Especially, the global south?

Eva Nagyfejeo
This is a very good question. I can mostly talk about the countries, the nine countries that I've participated in. Based on the nine countries, and these countries that I picked and presented, there were always some little fragmentation in the system. So, there was always lack of coordination, not enough resources. So, I don't think I seen a successfully implemented national cybersecurity awareness raising program, based on my experience, but I would be happy to look into that and come back to you with an answer, later on, thank you.

Enrico Calandro
Thank you, Eva.

Exactly. And I think that one of the main problems is this lack of coordination. So, most probably, there are a number of initiatives in the global south to raise awareness, but they're not properly coordinated. So, from a cyber maturity perspective, that's considered as a weakness, or a lowered stage of maturity. That doesn't mean that there aren't actually very valuable cyber awareness programs nationally, that maybe are conducted by civil society organizations, or by universities, but they're not coordinated. So, that's something that we need to take into account.

Another interesting question from Gabriel Nhinda, I don't know if Gabriel would like to ask the question yourself, or I can do it on your behalf?

Okay, I can ask this as well. So, from the research conducted, have you encountered countries in the global south that had awareness materials in local languages? This is something that you have mentioned.

Eva Nagyfejeo
Yes.

Enrico Calandro
Have you found material in the local in local languages?

Eva Nagyfejeo
Not that I'm aware of, for all the countries I've participated in, but I think, or I hope, that there are now some countries working on developing awareness raising materials, and and I'm sure that the international stakeholders, working together with governments, and I understand that this could be quite time consuming as well, to translate materials, as well. I remember, I think, in Brazil, that I've been to, and we have published the CMM report recently, they have a cyber maturity portal, which was not included in this paper, but they they have materials in Portuguese. But, in the countries that are in the paper, I'm not aware of awareness raising materials in the local language, but I will look into this again, and come back to you with a more specific answer. It's a very good question.

Enrico Calandro
Yeah, thank you. So, I've seen that actually, Carolin from the Global Cyber Security Capacity Center, she put in the chat a link to a campaign in Myanmar, which was translated in the local

language. And also, are the results on other toolkits. So, maybe you can have a look at that study, and there is also a South African one, which is translated in a couple of local languages. So, both links are in the in the chat.

Enrico Calandro
And I see another question, a very quick one from B K. Is Asia Pacific region included in the research?

Eva Nagyfejeo
Asia Pacific? Um, no, not at the moment. Because mostly I tried to take advantage of the opportunity that I've been participating in these countries, except the two, and we really tried to look at differences in geographical location. But, yeah, it would be great to look at, into those countries, as well. I think, as Carolin mentioned, there was a CMM review in Myanmar. And we hope that, in the future, there might be CMM reviews conducted in that region as well, so we can deliver more research and share our findings with the public.

Enrico Calandro
Thank you Eva.

I see Richard Hill has got his hand up. So Richard, would you like to take the floor?

Richard Hill
Yes, thank you. So, first of all, thank you very much, both for the presentation, but mostly for the substantive work. I think this is really excellent, clearly it's what's needed , and hopefully will help.

I wanted to comment on what you said Enrico, about the parliamentarians, and not knowing much about this, I can confirm that in Switzerland. We've had various laws passed, which we, ISOC Switzerland, think are unfortunate. And a couple of our members actually have taken the time to talk to parliamentarians, there are four or five who actually understand the issues, but they're completely swamped by people who have no understanding, and they get emotional, like, Oh, we have to protect the children, so we have to block websites, and stuff like that. Switzerland may be the worst case, because the parliament is part timers, and they don't really have experts that can help them, but I suspect that other countries are also pretty bad.

And then I wanted to make another comment, which goes rather to the content of the awareness. And there, I think, really, it's very good if you can go back to 2016 ISOC study, which I find excellent, which points out these market failures. I mentioned on the chat, the asymmetry of information, but the other one is externalities, people don't realize that my lack of security may not be a problem for me, but it may well be a problem for you. For example, you know, the credit card companies that don't protect enough, you know, they don't lose any money when a credit card gets stolen, but you do. And it's very well documented in that report. So, I think that report would be a good basis to develop some of the contents of the awareness building, but again, very well done, and thank you very much.

Enrico Calandro
Thanks, Richard, for your intervention, and also for sharing with us that report, that I've seen you placed in the chat, so if anybody would like to have a look at that, especially on the content side of this cyber awareness campaign, please refer to that.

We have a number of questions. So, thank you, it means that they are very engaging kind of panel. So, from Edward Millington, he's asking if there is any relationship in the CMM, in the national strategy? If the national strategy is linked to the national digital transformation programme, in the CMM? Is there any dimension that is investigating the relationship between these two programmes?

Eva Nagyfejeo
Thank you for the question. I'm just thinking now. At the moment, I don't think we have specific indicators, within this aspect. But actually, it's a really good point. And, actually, at the moment, we are working on revising the CMM. So, any suggestion is also very welcome, any feedback and comments, how we could improve the CMM, as well. We've been already doing extensive consultation in the past year, and we are hoping to publish by the end of this year. So, this is a really good point. And I'm going to take a note of that. Thank you.

Enrico Calandro
Thank you. Yeah, I agree. But probably, cyber security can somehow be seen as an extension of a broader digital transformation program. So, it's a very good point. Sofia Hunter is asking, What would you say are the main benefits of having a national cybersecurity awareness portal? I think it's a very interesting question. What are the benefits of this portal?

Eva Nagyfejeo
I think having a portal, I'm thinking about Brazil. Based on my experience in the countries I've been to, I had the opportunity. I think it was only Brazil which had an awareness raising portal in place, in Portuguese, at the time of the assessment, I'd been, part of 2018. And because, in the paper, at the time of the assessment, none of these countries had, and I think the benefit of

having the portal would be, you know, anybody who is interested, whether it's coming from private sector, academia, school children, women, they can just have this portal provided by the government, and they can just look at all the materials related to cybersecurity, seminars, courses, and if they want to educate the children, there could be cyber books for children, online programs, like also parenting controls, like how to control your kids' behavior online, what to do as a parent ,because we need to raise more awareness of it, and there is a generation growing up, who is very digital, and then there is the older generation, who are just getting more involved in this, and they need to learn, and these are new challenges, and they need to adapt to these digital challenges, and digital education, and make their children aware of the harms online, not just the benefits, and the convenience, that may come from the Internet, and using social media, and also, you know, talking about disinformation, issue programmes, and campaigns as well, and to make them become responsible that, who can decide what information is truthful, what information is trusted, and what they can see it with a critical eye, and see, okay, this -- and they have this resiliency in their mindset. So, it's a long term goal, it's not going to happen from one day to the other. But, I think, the government could be a very important driving force. So, if they recognize it, and work together with all the partners, listen to all the different stakeholders, and work together, hand in hand, I think it's a very good investment in the long run.

Enrico Calandro
Thank you. Yeah, that's a that's an excellent point. And, probably, also the value added of an international portal, is that actually, it could be translated in different local languages, right? That, as we have seen, we shared the link to the Cybil portal, where you can find a number of these guidelines and toolkits, but, of course, they're all in English. So, we need, somehow, to bridge that kind of linguistic barrier, and probably national portals are an effective way of doing that.

Just to go back to the comment on the research in Asia, there is need, probably then, to do a bit more of this research also in Asia, for instance, India, Pakistan, in Bangladesh, and other countries? Is there any plan of doing, of covering also that region, for CMM?

Eva Nagyfejeo
Yeah, I forgot to mention. There was a CMM Report -- I'm not sure if it's published -- but Myanmar and Bangladesh, we've been to Bangladesh, research team. And, I think, there are discussions to -- and Sri Lanka as well. And there are discussions, I think, to do CMM reviews, hopefully, in India, in the next years. But yeah, I can ask my colleagues, and provide more information, if anybody is interested to learn about it. But yeah, we are really hoping to cover that region as well, in in the next years, and hopefully, to do second assessment, as well, to see how the country progressed, in the past four years.

Enrico Calandro

Thank you. Maybe we can also place the link with all the CMM reviews conducted, here in the chat, so that people can just read them, and see all countries that have been covered, so far. And, as I was saying, unfortunately, not all reports are publicly available online, because some governments do not want to share the report at the end. So, in that case, unfortunately, it's not possible to to share that. But, on the map, you will see actually where the study was conducted.

Enrico Calandro

We still have a few minutes, so I actually have another question for you, Eva.

Specifically on, what I found very interesting is, also, as you said, that you have observed some cultural differences, right? Across these countries, on this cyber awareness program. And, I think, that's also the real value right of doing field research on these kind of topics. So, I'm just wondering, how would you develop then this research further, to try to highlight these geographical differences across countries? Do you think that there is any job, expanding your methodology? What would you recommend?

Eva Nagyfejeo

Oh, thank you very much for this question. I think, if anybody -- I hope they got some inspiration, I think there's still more could be done, in terms of research.

I would be, for instance, very interested to learn more about how the community leaders, or religious leaders, could be involved in, in cyber capacity building in those countries where they they have an important role. It would be also good to learn more about the culture, the mindset, how the people, the users, approach and think about cybersecurity issues, how they would react if they would become victims of cyber bullying, cyber abuse as well, and how this could be more integrated into awareness raising programme, how these cultural issues, or mindset issues, could be resolved in the long run, I assume it would be, go back to education, and training their mindset, from from primary school, and make them aware of the of the dangers out there, not just the good things about Internet, so, from primary school, and make them more responsible, and resilient. So, I think, awareness raising programmes and cyber education would go hand in hand, and, I think the cyber education side could be also explored. So, yeah, I just mentioned a few examples. But, of course, they are also more areas to to look at, and I hope this will help others to become more interested in, and do some research in this area.

Enrico Calandro

It's a very good invite, and I think that there are many opportunities, actually, of conducting research in this area, especially to understand the local realities, and the local context, of these cyber awareness campaigns. And the effectiveness. So, yeah, I would invite the participants, those are interested in this, maybe they can discuss that with you, as well as a follow up also with me, we might find opportunities to do research in this topic.

Now, to go at another level, so we're discussing the local reality, try to understand the local differences, and national differences. And you mentioned in your presentation, also, the role of international partners. We have seen that there are, actually, a number of stakeholders involved in these efforts, so that at an international level, you know, they play an important role. You mentioned the Global Forum on Cyber Expertise, which is trying to coordinate a number of cyber and capacity activities, globally. And you also placed the regional organizations, between the international and actors that are involved in cyber awareness campaign. So, do you see any specific role, especially maybe in the relationship with the national governments, how should they approach? How can they have the kind of role of coordinating these activities globally, while working nationally, in order to understand the national differences, and the peculiarity at the national level?

Eva Nagyfejeo

Yes, that's a very good question. Thanks very much, Enrico. I think, what role international stakeholders could play? I think they have a very important supporting role for the governments, and to help them, assist, in their awareness raising, to develop an awareness raising program. And, that's what we also trying to do, when we deploy the CMM, and work with the strategic and implementation partners in the country, to do with the CMM, to support the government, to realize what are the gaps that's missing in the country, in the cybersecurity maturity, where needs investment, whether it's the legislation, whether it's the strategy, whether it's the education, or whether it's the the technological aspects of the cybersecurity, at the organizational level. So, I think these CMM could -- it's more like, a facilitated self help. It's a self assessment for the country, and, working together with with the international stakeholders, I think they could be a complementary act, as a complementary support for the government. And I think it's important to involve them, and listen to them. Of course, it will be, in the end, the decision of the government, whether they would like to take their recommendations over, but at least listen to them, and decide to what extent they want to involve them. I think they deserve a chance to be heard, and be involved, because they helped a lot in capacity building, and they could foster synergies, and help to avoid duplication efforts, and overlaps, and we are all in this together. So, I think they are not, a country cannot really solve this problem alone. So, we are all interdependent, and you are the strongest and weakest link. So, if, in the region, you have a country which is really weak, so the cyber security, it affects the neighboring countries as well. So, you have to be open to this end, and involve those who have expertise, and work together, collaboratively, and not in a competitive way. So, that would be my personal opinion on that.

Enrico Calandro
Thank you, Eva. I agree, a perfect agree.

And, I've seen, in some instances, also bilateral kind of collaborations, between two governments, for instance, and that can be either north-south, but also south-south. So, those are other models as well that, in many cases, can work, and you know, different government entities can share experiences, and build the their own capacity while they are working together. So, for the bilateral aspect, I think it is important.

My final question, if there aren't other questions from the public, is then on your final recommendation, on then the review of the programmes, right? After the campaign has been done, has been conducted, you recommend then to try to review, to measure the effectiveness of the cyber awareness campaign? How would you recommend to do that? Because the CMM, as you will describe this [inaudible], and on cyber awareness? So, would you recommend to use the dimension on the CMM? Or would you need to develop specific metrics, or indicators, to measure the effectiveness? How would you go about that?

Eva Nagyfejeo
Oh, that's a very good question. Of course, the country's always welcome to use the CMM as a basis, but the country's also very welcome to, when it comes to metrics and surveys, to come up with their own version. And, when it comes to assessing the effectiveness of awareness raising campaigns, and this is where they could ask the support of international stakeholders, for instance, who have maybe experience already in other countries, and they could provide some advice on how to conduct these metrics and surveys. So, it could be a long term process, but it's very effective. And with the involvement of other stakeholders, with the private sector, within the country, I think it would be really good to have a measure to what extent the programs are effective, what's lacking, what needs to be changed or revised, or divert? Because some social groups are missing, or not enough, or so I think this is always good to self check. I was talking on behalf of the [inaudible], to self check yourself, like what you deliver, and services you provide for the country, is good enough? And, yeah, it's a multistakeholder approach that's needed. But I don't have an exact plan, how to do the metrics, but I think, with the involvement with others, stakeholders, international partners, they could really come up with good metrics as well.

Enrico Calandro
Thank you. Thank you for that. I am seeing another question on, if there are other approaches, other than the Cyber Maturity Model. And, yeah, I know that there are, and actually a task force within the Global Forum on Cyber Expertise is exploring this issue. So, they're actually working on trying to identify the different methodologies to measure capacity. So, the Cyber Maturity Model for nations is one of them, but there are others.

And actually, we have here with us, Carolin from the Global Cyber Security Capacity Center at Oxford, that she is leading that working group on the Global Forum on Cyber Expertise, so maybe she can share with us the other models that are there available, to measure maturity, cyber maturity.

Carolin Weiser Harris
Thank you, Enrico. Thank you for the question, which came from B K.

Carolin Weiser Harris
Yes, so there are several tools on the globe, which do similar things as we do. One is the Global Cybersecurity Index by the ITU, and that's, as it said, an index. They also look at several areas, some of the areas, a questionnaire sent out to GEIT members. And then there's a report I think, every year. You can find that also on the ITU website.

And the Cybil Portal, which was mentioned earlier, and this is complementary. We very close with the ITU. And then there's the Cyber Readiness Index, by the Potomac Institute. There's also E-Gov, by the E-Governance Academy in Estonia. It's called National Cyber Security Index. And there is from MITRE, a framework to assess cybersecurity. We are working on this overview document right now. It was by the GFCE, what Enrico could just mentioned, and so yeah, stay tuned via our Twitter account, on the Cybil Portal, or via the GFCE. Because it will be published early next year, and then you can see it, and have a better understanding what the different tools are.

Thank you.

Enrico Calandro
Thank you, Carol. That's I think that's a very interesting initiative because, as we said, there are a number of methodologies, and all these methodologies have been developed through, you know, multistakeholder participation, and the people are revising, reviewing them. So, lots of work has been put there, and you might use also, different methodologies based on your specific needs.

So, I see that we are now at one hour, and I don't see any other additional question on on this topic, but I believe it was a very interesting one. And we shared lots of information, and you can keep in touch both with me or with Eva, on this topic.

Eva, when will you publish the paper? Because it was submitted to a conference, is it already published, publicly available?

Eva Nagyfejeo
Yes, the paper was submitted and accepted by the CyberEdu conference, and I just got the email that said that it will be published this December. So, if all goes well, in December this paper will be published and available.

So, thank you very much for everyone's time and participation. And we are very happy that you were here.

Enrico Calandro
Thank you. And as I see Carolin also placed the link to the different assessment, so you can find actually the various tools on that link.

And now, I would give the floor back to Oscar for maybe his closing remarks.

Oscar Noe Avila
Okay, perfect.

Oscar Noe Avila
Thank you, Eva, and Enrico for sharing a all the information. And no, I have no further questions or comments.

So, again I would like to thank you, and also our audience, for joining us today.

And that's what I have. So, thank you so much, and I think that it is time to close the session.

Thank you Enrico and Eva, and Carolin as well.

Eva Nagyfejeo
Thank you very much.

Oscar Noe Avila
You're welcome.

Enrico Calandro
Thank you all

Oscar Noe Avila
Ciao.

Enrico Calandro
Bye bye.

Oscar Noe Avila
Bye.

ADDENDUM – Links from chat

- https://gcscc.ox.ac.uk/the-cmm
- https://gcscc.ox.ac.uk/events-0#collapse2289891
- https://future.internetsociety.org/2016/index.html
- https://cybilportal.org/tools/?_sft_themes=cyber-security-awareness
- https://www.linkedin.com/feed/update/urn:li:activity:6719935024008830977/
- https://www.linkedin.com/feed/update/urn:li:activity:6719934147583852544/
- https://gcscc.ox.ac.uk/cmm-reviews
- https://cybilportal.org/tools/?_sft_themes=assessments